REMARKS

Claims 30, 32-38, 40-45 and 47 to 50 remain in the application. The claims have been carefully reviewed with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present response.

Reconsideration is respectfully requested of the rejection of claims 30, 32-38, 40-45 and 47 to 50 as allegedly being unpatentable over U.S. Patent No. 6,226,744 to Murphy et al. in light of U.S. Patent No. 6,308,886 to Benson et al.

Applicant has carefully considered the comments of the Office Action and the cited references, and respectfully submits that claims 30, 32-38, 40-45 and 47 to 50 are patentable over the cited references for at least the following reasons.

The present invention relates to a system for allowing a user to complete a secure transaction over a network. The system includes at least a data card, a data card reader, a data processor and an application program. The data card contains information specific to the user, including authentication and personal information. The data card reader is adapted to access at least part of the information on the data card. The data processor is in communication with the data card reader and may be connected to the network. The application program is resident on the data processor, and configured to automatically prompt the user to enter the authentication information for comparison with the authentication information on the data card to allow the user to complete the secure transaction over the network using the user-specific information. Upon initial use of the data card, the user is prompted to initiate the data card by inputting the authentication information and the personal information for storage on the data card.

Murphy et al., as understood by Applicant, relates to a method and apparatus for authenticating users on a network using a smart card. The network includes a client computer and server computer, and the client computer contains a smart card reader. The client computer sends a request to the server to access restricted information stored within the server. The server sends a smart card interface module to the client computer, and requests an access code from a user to access the smart card. When the server receives the access code, the server accesses user information stored on the smart card utilizing the module and access code. The server compares the user information with authentication information available only to the server. If the user information matches the authentication information, the server grants the client computer access to restricted information.

Benson et al., as understood by Applicant, relates to a system for processing and/or issuing cards containing machine-readable information. The system may be housed in a terminal which includes an insertion port to accept a card from a user and further includes a hopper which stores a plurality of blank cards. The card, after issuance and/or processing may include human-readable data on the front surface, such as the name of the card issuer, the name of the person to whom the card is issued (recipient), an account number etc. The card may also include one or more magnetic stripes on the back surface for storage of machine-readable data. See Benson et al., Col. 4, lines 47-65.

The Office Action concedes that Murphy et al. fails to disclose or fairly suggest that upon initial use of the card the user is prompted to initiate the data card by inputting the authentication information and the personal information. The Office Action, however, states, "Benson et al. disclose a terminal for issuing and processing data bearing documents comprising: a control computer 266, wherein the operator instructs the computer to activate a PINpad PP for receiving a selected input or PIN on a keyboard KP, the PIN is selected during the initial used wherein the selected PIN is stored in the card." See Office Action, p.3. The Office Action further states that, in view of Benson's teachings, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to modify the system of Murphy et al. so that "operators(users)" could select their own PIN. See Office Action, p.3. Applicant respectfully disagrees.

Benson et al. discloses that the operator may send appropriate commands to the terminal via the mode switches 24 to initiate operation. If a PIN is to be selected, the operator may construct the control computer 266 to activate the PINpad PP for receiving a selected input or PIN on the keypad KP. The PIN may be encrypted and stored on the magnetic strip as an added security feature. See Benson et al., Col. 16, lines 38-52. Benson et al. further discloses that "[T]hereafter the operator may trigger the control computer 268 to initiate operation of the input hopper mechanism 34(inclusive of motor 39, the rollers 42 and the belts 44), for dispensing a blank card from the stacker 36 or the operator may manually insert a card through entry point E to be received in the receiving station." See Benson et al., Col. 16, lines 52-58.

The operator of Benson et al., as understood by Applicant, however, is not the user of the card, the recipient, but the operator of the system for issuing the card. See Benson et al., Col. 4, lines 49-50.

Even if the operator of Benson et al. were to be considered the user, Benson et al. discloses entry of a PIN to be stored on the card prior to utilization of the card. In contrast, in the present application, upon initial use of the card, the user is prompted to initiate the data card by inputting the authentication information and the personal information into the data processor for storage on the data card.

In addition, in the presently claimed invention, the user inputs the authentication information and the personal information upon an initial use of the card. Benson et al. discloses that the operator may enter a PIN, however, Benson et al. does not show or suggest entering the authentication information <u>and</u> the personal information upon an initial use of the data card.

As noted above, the Office Action further contends that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Murphy et al. so that operators could select their own pin. Applicant respectfully disagrees.

Murphy et al. relates to a method and apparatus for authenticating users on a network using a smart card, whereas, Benson et al. relates to a system for issuing and processing data-bearing documents or cards. In Murphy et al., the smart cards used to authenticate users are issued by a Certified Authority (CA) and store information provided exclusively by the CA. See Murphy et al., Col. 5, lines 53-56.

Murphy et al., Benson et al. and the other cited art fail to suggest combining the feature of allowing the operator to enter a PIN disclosed in Benson et al. with the system for authenticating users of Murphy et al. In fact, Murphy et al. specifically teaches that the information stored on the smart card is to be provided by the CA, not by the user.

Accordingly, it is respectfully submitted that it would not have been obvious to incorporate the feature of allowing an operator to enter a PIN to be saved on a data-bearing card from Benson et al. into the system for authenticating users of Murphy et al.

With regard to the arguments presented in Applicant's December 15, 2003 Amendment, the Office Action indicates that Applicant's arguments have been considered, but are considered to be moot in light of the new grounds for rejection. Applicant respectfully disagrees.

As stated in the December 15, 2003 Amendment, the authentication module of Murphy et al. initiates a download of a smart card interface module to the client computer when the authentication determines that the smart card is present. Thus, as understood by Applicant, the interface module is not located on the client computer, but is instead downloaded from a remote database.

While Benson et al. may disclose that a PIN may be entered by the operator and stored on the data-bearing card, Benson et al. fails to disclose or to suggest an application program resident on the data processor and configured to automatically prompt the user to enter the authentication information for comparison with the authentication information stored on the data card in order to authorized the user.

In contrast, in the presently claimed invention, an application program is resident on the data processor and is configured to automatically prompt the user to enter the authentication information for comparison with the authentication information stored on the data card in order to authorize the user. See present specification, p. 13, lines 19-21.

Furthermore, as understood by Applicant, the authentication apparatus and method of Murphy et al. are directed to allowing access to information stored on the server. See Murphy et al., Col. 3, lines 31-45; Col. 6, lines 43-49. The system for issuing and processing data-bearing documents of Benson et al., as understood by Applicant, is directed to a system for processing and/or issuing a card containing machine-readable information. See Benson et al., Col. 4, lines 38-40.

The computer system of the presently claimed invention, however, allows a user to complete a secure transaction over the network using the information specific to the user when authorized following a match of the authentication information by the application program. See present specification, p. 17, lines 12-16.

Accordingly, it is respectfully submitted that neither Murphy et al. nor Benson et al. teach or suggest a computer system for allowing a user to complete a secure transaction over a network, comprising a data card which contains information specific to the user, including authentication information and personal information; a data card reader, a data processor, and an application program resident on the data processor and configured to automatically prompt the user to enter the authentication information for comparison with the authentication information stored on the data card, in order to authorize the user following a match thereof to complete the secure transaction over the network using the information specific to the user, wherein upon initial use of the data card the user is prompted to initiate the data card by inputting the authentication information and the personal information into the data processor for storage on the data card, as described above and as recited in independent claim 30.

Accordingly, for at least the reasons mentioned above, it is respectfully submitted that independent claim 30, and the claims depending therefrom, are patentable over the cited art.

Independent claims 38 and 44, and the claims depending therefrom, are believed to be patentable over the cited art for at least similar reasons.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited art there is a basis for such disagreement.

The Office is hereby authorized to charge any fees which may be required in connection with this Request For Reconsideration and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

Dated: August 20, 2004

Norman H. Zivin
Reg. No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036
(212)278-0400
Attorney for Applicant

I hereby certify that this paper is being deposited this date with the U.S. Postal Service as first class mail addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

8/20/04

Norman H. Zivin
Reg. No. 25,3855

Date